CLAIMS

1. A method comprising:

establishing a session with a client;

receiving a request from the client;

determining whether the session is authenticated;

in an event that the session is not authenticated, persisting the request from the client as a pending request; and

in an event that the session is subsequently authenticated, processing the pending request.

2. The method of claim 1 wherein the determining comprises verifying an authentication token associated with the client.

3. The method of claim 2 wherein the verifying comprises verifying that the authentication token has not timed out.

4. The method of claim 2 wherein the authentication token is a cookie stored by the client.

5. The method of claim 2 wherein the authentication token is part of the request received from the client.

6. The method of claim 2 wherein the authentication token is encrypted.

7. The method of claim 1 wherein persisting the request comprises storing the request in a file.

8. The method of claim 1 wherein persisting the request comprises storing the request in a database.

9. The method of claim 1 further comprising, after persisting the request, directing the client to authenticate the session.

10. The method of claim 9 wherein directing the client to authenticate the session comprises:

directing the client to a login module; and

directing the client to an address associated with the pending request.

11. The method of claim 10 wherein the address associated with the pending request is a URL.

12. A method comprising:

establishing a session with a server;

submitting a request to the server;

receiving an indication that the session is not authenticated;

obtaining a session authentication; and

receiving an indication that the request has been processed.

13. A system comprising:

an authentication verifier configured to determine whether a session associated with a client is authorized;

a client interface configured to receive a request from the client;

a pending request store configured to maintain the request in an event that the session is not authorized; and

a processing unit configured to process the request that is maintained in an event that the session is authorized.

14. The system of claim 13 further comprising an authentication redirect generator configured to generate an instruction to redirect the client to obtain authorization for the session.

15. The system of claim 14 wherein the instruction is a URL.

16. The system of claim 14 wherein the authorization is an authentication token.

17. An application server comprising the system as recited in claim 13.

18. A system comprising:

a client interface configured to receive a request from a client;

an authentication token verifier configured to determine whether an authentication token associated with the client is valid;

a pending request store configured to store the request in an event that the authentication token associated with the client is not valid; and

an authentication redirect generator configured to generate an instruction to redirect the client to obtain a valid authentication token.

19. The system of claim 18 wherein the authentication token verifier is further configured to determine whether the authentication token has expired.

20. The system of claim 18 wherein the authentication redirect generator is further configured to direct the client to access the request that is stored.

21. The system of claim 18 wherein the pending request store is a database.

22. A system comprising:

means for receiving a request from a client;

means for determining whether an authentication token associated with the client is valid;

means for storing the request in an event that the authentication token is not valid; and

means for generating an instruction to redirect the client to obtain a valid authentication token.

23. A system comprising:

a client;

an application server configured to:

receive a request from the client;

maintain the request as a pending request in an event that the client is not authenticated; and

direct the client to obtain authentication;

the client being configured to obtain authentication from an authentication entity in response to direction from the application server, and the client further configured to access the pending request; and

upon client access to the pending request, the application server being further configured to process the pending request.

24. The system of claim 23 wherein the application server and the authentication entity are implemented as one server.

25. One or more computer-readable media comprising computer executable instructions that, when executed, direct a computing system to:

receive a request from a client;

determine whether the client is authenticated;

in an event that the client is not authenticated, persist the request; and

in an event that the client is subsequently authenticated, process the request that is persisted.

26. The one or more computer-readable media of claim 25 further comprising computer executable instructions that, when executed, direct a computing system to:

in the event that the client is not authenticated,

redirect the client to obtain authentication; and

direct the client to the request that is persisted.

27. One or more computer-readable media comprising computer executable instructions that, when executed, direct a computing system to:

receive a request from a client;

determine whether an authentication token associated with the client is valid;

store the request if the authentication token is not valid; and

generate an instruction to redirect the client.

28. The one or more computer-readable media of claim 27 wherein the instruction comprises an instruction to redirect the client to obtain a valid authentication token.

29. The one or more computer-readable media of claim 28 wherein the instruction further comprises an instruction to redirect the client to the request that is stored upon the client obtaining the valid authentication token.